Topic 5 –

The multiplicative structure of $\mathbb{Z}_n$

Def: Let $n \in \mathbb{Z}$ with $n \geq 2$.
Let $\overline{x}, \overline{y} \in \mathbb{Z}_n$.
We say that $\overline{x}$ and $\overline{y}$ are <u>multiplicative inverses</u> in $\mathbb{Z}_n$ if $\overline{x} \cdot \overline{y} = \overline{y} \cdot \overline{x} = 1$.

Ex: $\mathbb{Z}_{10} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\}$

In $\mathbb{Z}_{10}$,

$$\overline{3} \cdot \overline{7} = \overline{21} = \overline{1}$$

$$\boxed{\begin{array}{c} 21 \equiv 1 \pmod{10} \\ \hline 21 - 10 - 10 = 1 \end{array}}$$

So, $\overline{3}$ and $\overline{7}$ are multiplicative inverses in $\mathbb{Z}_{10}$

In $\mathbb{Z}_{10}$,

$$\overline{9}\cdot\overline{9} = \overline{81} = \overline{1}$$

$$\boxed{\begin{array}{l} 81 - 8\cdot 10 = 1 \\ 81 \equiv 1 \pmod{10} \end{array}}$$

So, $\overline{9}$ is its own multiplicative inverse in $\mathbb{Z}_{10}$.

Note that $\overline{2}$ has no inverse in $\mathbb{Z}_{10}$ because:

$$\left.\begin{array}{l}
\overline{2}\cdot\overline{0} = \overline{0} \neq \overline{1} \\
\overline{2}\cdot\overline{1} = \overline{2} \neq \overline{1} \\
\overline{2}\cdot\overline{2} = \overline{4} \neq \overline{1} \\
\overline{2}\cdot\overline{3} = \overline{6} \neq \overline{1} \\
\overline{2}\cdot\overline{4} = \overline{8} \neq \overline{1} \\
\overline{2}\cdot\overline{5} = \overline{10} = \overline{0} \neq \overline{1} \\
\overline{2}\cdot\overline{6} = \overline{12} = \overline{2} \neq \overline{1} \\
\overline{2}\cdot\overline{7} = \overline{14} = \overline{4} \neq \overline{1} \\
\overline{2}\cdot\overline{8} = \overline{16} = \overline{6} \neq \overline{1} \\
\overline{2}\cdot\overline{9} = \overline{18} = \overline{8} \neq \overline{1}
\end{array}\right\}$$

There is no $\overline{x}$ in $\mathbb{Z}_{10}$ with $\overline{2}\cdot\overline{x} = \overline{1}$.

Thus, $\overline{2}$ has no multiplicative inverse in $\mathbb{Z}_{10}$

Lemma: (HW 5 #15)
Let $n \in \mathbb{Z}$ with $n \geq 2$.
Let $a, b \in \mathbb{Z}$.
If $a \equiv b \pmod{n}$,
then $\gcd(a, n) = \gcd(b, n)$

$\boxed{\text{proof}}$: Suppose $a \equiv b \pmod{n}$.
Then, $a - b = qn$ for some $q \in \mathbb{Z}$.
Let $d = \gcd(a, n)$ and $d' = \gcd(b, n)$

Goal: Show $d = d'$.

Step 1: Let's show $d' \leq d$.
Since $d' = \gcd(b, n)$, we know
$d' \mid b$ and $d' \mid n$.
So, $b = d'k_1$ and $n = d'k_2$, where $k_1, k_2 \in \mathbb{Z}$.
Then, $a = qn + b = q\,d'k_2 + d'k_1$
$= d'[qk_2 + k_1]$.

So, $d' | a$.

Thus, $d' | a$ and $d' | n$.

Thus, d' is a positive common divisor of a and n.

But, $d = \gcd(a, n)$.

So, $d' \leq d$

<u>Step 2:</u> Let's show $d \leq d'$.

Since $d = \gcd(a, n)$ we know $d | a$ and $d | n$.

Thus, $a = dk_3$ and $n = dk_4$ for $k_3, k_4 \in \mathbb{Z}$.

So, $b = a - qn = dk_3 - qdk_4$
$= d[k_3 - qk_4]$

Therefore, $d | b$.

Thus, $d \mid b$ and $d \mid n$.

So, d is a positive common multiple of b and n.

Since $d' = \gcd(b, n)$ we must have $d \leq d'$.

By step 1 and step 2,

$d = d'$. $\blacksquare$

We want to determine which elements of $\mathbb{Z}_n$ have a multiplicative inverse.

Last time: Let $a, b, n \in \mathbb{Z}$ with $n \geq 2$. Suppose $a \equiv b \pmod{n}$. Then, $\gcd(a,n) = \gcd(b,n)$.

Why do we need this?

Suppose $\bar{a}, \bar{b} \in \mathbb{Z}_n$ and $\bar{a} = \bar{b}$. Then $a \equiv b \pmod{n}$.
So, $\gcd(a,n) = \gcd(b,n)$.

Ex: $n = 3$, $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$
$a = 2$, $b = 8$, $\bar{2} = \bar{8}$ and $\gcd(2,3) = 1 = \gcd(8,3)$

This makes it so the next Theorem makes sense.

Theorem: Let $a, n \in \mathbb{Z}$ with $n \geq 2$. Then, $\bar{a}$ has a multiplicative inverse in $\mathbb{Z}_n$ iff $\gcd(a,n) = 1$.

Moreover, if $\bar{a}$ has a multiplicative inverse, then the inverse is unique.

Note: The above thm makes sense since if $\bar{a} = \bar{b}$ then $\gcd(a,n) = \gcd(b,n)$

proof:

($\Longrightarrow$) Suppose $\bar{a}$ has a multiplicative inverse in $\mathbb{Z}_n$.

Thus, there exists $\bar{b} \in \mathbb{Z}_n$ where

$$\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a} = 1.$$

Let $d = \gcd(a,n)$.

We want to show that $d = 1$.

Let's show $d>1$ leads to a contradiction.

Suppose $d>1$.

Let $c = \frac{n}{d}$. ← $c \in \mathbb{Z}$ since $d \mid n$

Recall that $d = \gcd(a,n)$.

So, $d \mid n$.

Thus, $1 < d \leq n$.

Then, $1 \leq \frac{n}{d} < n$

divide $d \leq n$ by d

$d > 1$

So, $1 \leq c < n$.

Thus, $\overline{c} \neq \overline{0}$ in $\mathbb{Z}_n = \{\overline{0}, \underbrace{\overline{1}, \overline{2}, \ldots, \overline{n-1}}_{\overline{c} \text{ is one of these}}\}$

But also,

$$\overline{c} = \overline{\left(\frac{n}{d}\right)} = \overline{\left(\frac{n}{d}\right)} \cdot \overline{1} = \overline{\left(\frac{n}{d}\right)} \cdot \overline{a}\,\overline{b}$$

$\overline{n} = \overline{0}$ in $\mathbb{Z}_n$

$$= \overline{\left(\frac{na}{d}\right)}\,\overline{b} = \overline{\left(n \cdot \frac{a}{d}\right)} \cdot \overline{b} = \overline{n}\,\overline{\left(\frac{a}{d}\right)}\,\overline{b} = \overline{0}$$

↑ $\frac{a}{d} \in \mathbb{Z}$ because $d \mid a$

Thus, $\overline{c} \neq \overline{0}$ and $\overline{c} = \overline{0}$.

Contradiction.

So, $d = \gcd(a,n) = 1$.

($\Leftarrow$) Suppose $\gcd(a,n) = 1$.

We want to show that $\overline{a}$ has a multiplicative inverse in $\mathbb{Z}_n$.

Since $\gcd(a,n) = 1$ there exist $x_0, y_0 \in \mathbb{Z}$ where

$$ax_0 + ny_0 = 1.$$

Thus in $\mathbb{Z}_n$ we have $\overline{ax_0 + ny_0} = \overline{1}$.

So in $\mathbb{Z}_n$ we have $\overline{ax_0} + \overline{ny_0} = \overline{1}$.

Thus in $\mathbb{Z}_n$ we have $\overline{a}\,\overline{x_0} + \underbrace{\overline{n}\,\overline{y_0}}_{\boxed{\overline{0}}} = \overline{1}$.

In $\mathbb{Z}_n$ we know $\overline{n} = \overline{0}$.

Thus in $\mathbb{Z}_n$, $\overline{a}\,\overline{x_0} = \overline{1}$.

So, $\overline{a}$ has a multiplicative inverse $\overline{x_0}$ in $\mathbb{Z}_n$.

Let's now prove the Moreover part of the theorem.

Suppose $\bar{a}$ has a multiplicative inverse in $\mathbb{Z}_n$.

We want to show this inverse is unique.

Suppose $\bar{b}_1, \bar{b}_2 \in \mathbb{Z}_n$ are multiplicative inverses of $\bar{a}$.

Then, $\bar{a}\,\bar{b}_1 = \bar{b}_1\,\bar{a} = \bar{1}$ and
$\bar{a}\,\bar{b}_2 = \bar{b}_2\,\bar{a} = \bar{1}$.

It follows that

$$\bar{b}_1 = \bar{b}_1 \cdot \bar{1} = \bar{b}_1 \underbrace{\left(\bar{a}\,\bar{b}_2\right)}_{\bar{1}} = \underbrace{\left(\bar{b}_1\,\bar{a}\right)}_{\bar{1}} \bar{b}_2$$

$$= \bar{1} \cdot \bar{b}_2 = \bar{b}_2$$

Thus, $\bar{b}_1 = \bar{b}_2$ and the multiplicative inverse is unique $\blacksquare$

Def: Let $n \in \mathbb{Z}$ with $n \geq 2$.

Define

$$\mathbb{Z}_n^\times = \left\{ \bar{a} \in \mathbb{Z}_n \;\middle|\; \begin{array}{l}\bar{a} \text{ has a} \\ \text{multiplicative inverse}\end{array} \right\}$$
$$= \left\{ \bar{a} \in \mathbb{Z}_n \;\middle|\; \gcd(a,n) = 1 \right\}$$

Notation: If $\bar{a} \in \mathbb{Z}_n^\times$ then we denote its multiplicative inverse by $\bar{a}^{-1}$.

We can do this because the inverse is unique

Ex:

$$\mathbb{Z}_{10} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}$$

$\gcd(0,10) = 10 \neq 1$

$\gcd(1,10) = 1$

$\gcd(2,10) = 2 \neq 1$

$\gcd(3,10) = 1$

$\gcd(4,10) = 2 \neq 1$

$\gcd(5,10) = 5 \neq 1$

$\gcd(6,10) = 2 \neq 1$

$\gcd(7,10) = 1$

$\gcd(8,10) = 2 \neq 1$

$\gcd(9,10) = 1$

Thus,

$$\boxed{\mathbb{Z}_{10}^{\times} = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}}$$

$\bar{1} \cdot \bar{1} = \bar{1}$ ← $\bar{1}^{-1} = \bar{1}$

$\bar{3} \cdot \bar{7} = \bar{1}$ ← $\bar{3}^{-1} = \bar{7}$ or $\bar{7}^{-1} = \bar{3}$

$\bar{9} \cdot \bar{9} = \bar{1}$ ← $\bar{9}^{-1} = \bar{9}$

we calculated these on Monday

Ex:

gcd(0,15) = 15 ≠ 1 gcd(2,15) = 1

$$\mathbb{Z}_{15} = \{ \cancel{\overline{0}}, \overline{1}, \overline{2}, \cancel{\overline{3}}, \overline{4}, \cancel{\overline{5}}, \cancel{\overline{6}}, \overline{7}, \overline{8}, \cancel{\overline{9}}, \cancel{\overline{10}}, \overline{11}, \cancel{\overline{12}}, \overline{13}, \overline{14} \}$$

gcd(1,15) = 1

gcd(12,15) = 3 gcd(3,15) = 3 ≠ 1

gcd(9,15) = 3 ≠ 1

$$\boxed{\begin{aligned} \mathbb{Z}_{15}^{\times} &= \{ \overline{a} \in \mathbb{Z}_{15} \mid \gcd(a,15) = 1 \} \\ &= \{ \overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14} \} \end{aligned}}$$

Let's find the inverses:

$\overline{1} \cdot \overline{1} = \overline{1}$

$\overline{2} \cdot \overline{8} = \overline{16} = \overline{1}$

$\overline{4} \cdot \overline{4} = \overline{16} = \overline{1}$

$\overline{11} \cdot \overline{11} = \overline{121} = \overline{1}$

$\overline{7} \cdot \overline{13} = \overline{91} = \overline{1}$

$\overline{14} \cdot \overline{14} = \overline{196} = \overline{1}$

$$\begin{array}{r} 6 \\ 15 \overline{\smash{)}91} \\ -90 \\ \hline 1 \end{array} \qquad \begin{array}{r} 13 \\ 15 \overline{\smash{)}196} \\ -195 \\ \hline 1 \end{array} \qquad \begin{array}{r} 8 \\ 15 \overline{\smash{)}121} \\ -120 \\ \hline 1 \end{array}$$

Thus,

$\overline{1}^{-1} = \overline{1}$ $\quad \overline{7}^{-1} = \overline{13}$ $\quad \overline{13}^{-1} = \overline{7}$

$\overline{2}^{-1} = \overline{8}$ $\quad \overline{8}^{-1} = \overline{2}$ $\quad \overline{14}^{-1} = \overline{14}$

$\overline{4}^{-1} = \overline{4}$ $\quad \overline{11}^{-1} = \overline{11}$

We will show next time that $\mathbb{Z}_n^\times$ is closed under multiplication.

4550 info:

$\mathbb{Z}_n$ is a group under $+$

$\mathbb{Z}_n^\times$ is a group under $\cdot$

Recall:

$$\mathbb{Z}_n^{\times} = \{ \bar{a} \in \mathbb{Z}_n \mid \bar{a} \text{ has a multiplicative inverse} \}$$

$$= \{ \bar{a} \in \mathbb{Z}_n \mid \gcd(a,n) = 1 \}$$

Ex:

$$\mathbb{Z}_{10}^{\times} = \{ \bar{1}, \bar{3}, \bar{7}, \bar{9} \}$$

$$\mathbb{Z}_5^{\times} = \{ \bar{1}, \bar{2}, \bar{3}, \bar{4} \}$$

Def: Let a, b be positive integers. We say that a and b are relatively prime if $\gcd(a,b) = 1$

Ex: Let p be a prime. Then,

$$\mathbb{Z}_p = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1} \}$$

$$\mathbb{Z}_p^{\times} = \{ \bar{1}, \bar{2}, \ldots, \overline{p-1} \}$$

$\gcd(0, p) = p$

If $1 \le x \le p-1$, $\gcd(x, p) = 1$

<u>Theorem:</u> Let $n \in \mathbb{Z}$, $n \geq 2$.
Then, $\mathbb{Z}_n^\times$ is closed under multiplication.
That is, if $\bar{a}, \bar{b} \in \mathbb{Z}_n^\times$ then

$$\bar{a} \cdot \bar{b} \in \mathbb{Z}_n^\times.$$

<u>proof:</u> Let $\bar{a}, \bar{b} \in \mathbb{Z}_n^\times$
We want to show that $\bar{a} \cdot \bar{b} = \overline{ab}$
is also in $\mathbb{Z}_n^\times$.

Since $\bar{a}, \bar{b} \in \mathbb{Z}_n^\times$ we know there
exists $\bar{a}^{-1}, \bar{b}^{-1} \in \mathbb{Z}_n^\times$ with

$$\bar{a}(\bar{a}^{-1}) = (\bar{a}^{-1})\,\bar{a} = \bar{1}$$

and $\bar{b}(\bar{b}^{-1}) = (\bar{b}^{-1})\bar{b} = \bar{1}$.

I claim that $(\bar{a}\bar{b})^{-1} = (\bar{b}^{-1})(\bar{a}^{-1})$.
Let's check this.

We have

$$(\bar{a}\,\bar{b})(\bar{b}^{-1}\bar{a}^{-1}) = \bar{a}\,\underbrace{\bar{b}\,\bar{b}^{-1}}_{\bar{1}}\,\bar{a}^{-1} = \bar{a}\,\bar{a}^{-1} = 1$$

and

$$(\bar{b}^{-1}\bar{a}^{-1})(\bar{a}\,\bar{b}) = \bar{b}^{-1}\,\underbrace{\bar{a}^{-1}\bar{a}}_{\bar{1}}\,\bar{b} = \bar{b}^{-1}\bar{b} = \bar{1}.$$

Thus,

$$(\bar{a}\,\bar{b})^{-1} = \bar{b}^{-1}\cdot\bar{a}^{-1}.$$

So, $\bar{a}\,\bar{b}$ has a multiplicative inverse and thus $\bar{a}\,\bar{b} \in \mathbb{Z}_n^{\times}$.

So, $\mathbb{Z}_n^{\times}$ is closed under multiplication $\blacksquare$

<u>Question:</u> When can an element in $\mathbb{Z}_n^\times$ be its own multiplicative inverse?

We will answer this question when n is prime.

<u>Ex:</u> $\mathbb{Z}_5^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

$\overline{1} \cdot \overline{1} = \overline{1}$ ⟵ $\overline{1}^{-1} = \overline{1}$

$\overline{2} \cdot \overline{2} = \overline{4}$ ⟵ $\overline{2}^{-1} \neq \overline{2}$

$\overline{3} \cdot \overline{3} = \overline{9} = \overline{4}$ ⟵ $\overline{3}^{-1} \neq \overline{3}$

$\overline{4} \cdot \overline{4} = \overline{16} = \overline{1}$ ⟵ $\overline{4}^{-1} = \overline{4}$

In $\mathbb{Z}_5$, $\overline{1}$ and $\overline{4}$ are equal to their multiplicative inverse.

Another way to see why $\overline{4}^{-1} = \overline{4}$ is because $\overline{4} = \overline{-1}$ and so $\overline{4} \cdot \overline{4} = \overline{-1} \cdot \overline{-1} = \overline{1}$

Theorem: Let p be a prime.
If $\overline{x} \in \mathbb{Z}_p^\times$ and $\overline{x}^2 = \overline{1}$,
then $\overline{x} = \overline{1}$ or $\overline{x} = \overline{-1} = \overline{p-1}$

That is, the only elements of $\mathbb{Z}_p^\times$ that are equal to their multiplicative inverse are $\overline{1}$ and $\overline{-1} = \overline{p-1}$.

proof:
Let $\overline{x} \in \mathbb{Z}_p^\times$ where $x \in \mathbb{Z}$.
Suppose $\overline{x}^2 = \overline{1}$.
Then $x^2 \equiv 1 \pmod{p}$.
So, $p \mid (x^2 - 1)$.
Thus, $p \mid (x-1)(x+1)$.
Since p is prime we know

$$p \mid (x-1) \text{ or } p \mid (x+1).$$

Magical property of primes
p is a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$

Either $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$
Therefore, $\overline{x} = \overline{1}$ or $\overline{x} = \overline{-1} = \overline{p-1}$ in $\mathbb{Z}_p^\times$ ▨

<u>Note:</u> The previous theorem is not true if n is not prime.

For example, we saw last time that

$$\mathbb{Z}_{15}^{\times} = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$$

and

$$\overline{1}^{-1} = \overline{1}$$

$$\left.\begin{array}{l} \overline{4}^{-1} = \overline{4} \\ \overline{11}^{-1} = \overline{11} \end{array}\right\} \text{extra ones not in previous thm}$$

$$\overline{14}^{-1} = \overline{14}$$

Ex: $p=13$ is a prime. Then,

$$\mathbb{Z}_{13}^{\times} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}\}$$

Check out what happens when we multiply all the elements of $\mathbb{Z}_{13}^{\times}$ together.

$$\overline{12!} = \overline{1}\cdot\overline{2}\cdot\overline{3}\cdot\overline{4}\cdot\overline{5}\cdot\overline{6}\cdot\overline{7}\cdot\overline{8}\cdot\overline{9}\cdot\overline{10}\cdot\overline{11}\cdot\overline{12}$$

$$= \overline{1}\cdot(\overline{2}\cdot\overline{7})(\overline{3}\cdot\overline{9})(\overline{4}\cdot\overline{10})(\overline{5}\cdot\overline{8})(\overline{6}\cdot\overline{11})\cdot\overline{12}$$

these are inverses

these are there own inverses

$\overline{12} = \overline{-1} = \overline{p-1} = \overline{13-1}$

$$= \overline{1}\cdot(\overline{14})\cdot(\overline{27})\cdot(\overline{40})\cdot(\overline{40})\cdot(\overline{66})\cdot\overline{12}$$

$$= \overline{1}\cdot\overline{1}\cdot\overline{1}\cdot\overline{1}\cdot\overline{1}\cdot\overline{1}\cdot\overline{12}$$

$$= \overline{12} = \overline{-1}$$

$\boxed{12 \equiv -1 \pmod{13}}$

$14 \equiv 1 \pmod{13}$
$27 \equiv 1 \pmod{13}$
$40 \equiv 1 \pmod{13}$
$66 \equiv 1 \pmod{13}$

multiples of 13:
13, 26, 39, 52, 65, 78, ...

$\boxed{\text{Theorem (Wilson's Theorem)}}$:

Let p be a prime.
Then,

$$\overline{(p-1)!} = \overline{-1}$$

in $\mathbb{Z}_p^\times$.

$\boxed{(p-1)! \equiv -1 \pmod{p}}$

Last time

$p = 13$

$\overline{12!} = \overline{-1}$

in $\mathbb{Z}_{13}^\times$

That is, if you multiply all of the elements of $\mathbb{Z}_p^\times$ together then you get

$$\underbrace{\overline{1} \cdot \overline{2} \cdot \overline{3} \cdots \overline{p-1}}_{\overline{(p-1)!}} = \overline{-1}$$

in $\mathbb{Z}_p^\times$.

proof:

If $p=2$, then

$$\overline{(p-1)!} = \overline{(2-1)!} = \overline{1!} = \overline{1} = \overline{-1}$$

in $\mathbb{Z}_2^\times = \{\overline{1}\}$.

$\boxed{1 \equiv -1 \pmod{2}}$

So the theorem is true when $p=2$.

Suppose now that p is odd.

Note that (from our Monday class) if $\overline{x} \in \mathbb{Z}_p^\times$ with $2 \leq x \leq p-2$ then there exists a unique $\overline{y} \in \mathbb{Z}_p^\times$ with $2 \leq y \leq p-2$ and $y \neq x$ and $\overline{y} = \overline{x}^{-1}$

[This is because we showed the only elements of $\mathbb{Z}_p^\times = \{\overline{1}, \overline{2}, \ldots, \overline{p-2}, \overline{p-1}\}$ which equal their own inverse are $\overline{1}$ and $\overline{p-1}$]

Thus, by pairing elements in the following product with their unique inverses (like in the $p=13$ example from Monday) we get:

$$\overline{(p-1)!} = \overline{1} \cdot \underbrace{\overline{2} \cdot \overline{3} \cdots \overline{p-2}}_{\text{every element in this range cancels with its inverse}} \cdot \overline{p-1}$$

$$= \overline{1} \cdot \overline{p-1}$$

$$= \overline{p-1}$$

$$= \overline{-1}$$

$p-1 \equiv -1 \pmod{p}$

in $\mathbb{Z}_p^{\times}$ $\blacksquare$

Def: Let n be an integer with $n \geq 2$.
Define the <u>Euler phi-function</u> (or Euler totient function) by the formula

$$\varphi(n) = |\mathbb{Z}_n^\times|$$

size of the set $\mathbb{Z}_n^\times$

$|S|$ ← size of set S

So,

$$\varphi(n) = \left| \left\{ \bar{x} \in \mathbb{Z}_n \;\middle|\; \gcd(x,n) = 1 \right\} \right|$$

$$= \left| \left\{ x \in \mathbb{Z} \;\middle|\; \begin{array}{l} 0 \leq x \leq n-1 \\ \gcd(x,n) = 1 \end{array} \right\} \right|$$

Ex:

$$\varphi(2) = |\mathbb{Z}_2^\times| = |\{\overline{1}\}| = 1$$

$$\varphi(3) = |\mathbb{Z}_3^\times| = |\{\overline{1}, \overline{2}\}| = 2$$

$$\varphi(4) = |\mathbb{Z}_4^\times| = |\{\overline{1}, \overline{3}\}| = 2$$

$$\boxed{\mathbb{Z}_4 = \{\cancel{\overline{0}}, \overline{1}, \cancel{\overline{2}}, \overline{3}\}}$$

$$\varphi(5) = |\mathbb{Z}_5^\times| = |\{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}| = 4$$

$$\varphi(6) = |\mathbb{Z}_6^\times| = |\{\overline{1}, \overline{5}\}| = 2$$

$$\boxed{\mathbb{Z}_6 = \{\cancel{\overline{0}}, \overline{1}, \cancel{\overline{2}}, \cancel{\overline{3}}, \cancel{\overline{4}}, \overline{5}\}}$$

$\gcd(4,6) = 2 \neq 1$

$\gcd(5,6) = 1$

$\gcd(2,6) = 2 \neq 1$

$\vdots \qquad \vdots$

$$\varphi(10) = |\mathbb{Z}_{10}^\times| = |\{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}| = 4$$

Theorem:

① If p is a prime, then $\varphi(p) = p-1$.

② If p is a prime and k is a positive integer, then

$$\varphi(p^k) = p^k - p^{k-1}$$

③ If a and b are positive integers with $\gcd(a,b)=1$ then $\varphi(ab) = \varphi(a)\varphi(b)$

[we say that φ is a multiplicative function because of this property]

④ If $n = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ is the prime factorization of n, then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_n}\right)$$

We won't prove this theorem

<u>Ex:</u> Calculate $|\mathbb{Z}_{360}^{\times}|$.

$$
\begin{aligned}
|\mathbb{Z}_{360}^{\times}| &= \varphi(360) \\
&= \varphi(2^3 \cdot 3^2 \cdot 5) \\
&\overset{4}{=} 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) \\
&= 360\left(\frac{2-1}{2}\right)\left(\frac{3-1}{3}\right)\left(\frac{5-1}{5}\right) \\
&= 360\left(\frac{1}{\cancel{2}}\right)\left(\frac{\cancel{2}}{3}\right)\left(\frac{4}{5}\right) \\
&= 2^3 \cdot \cancel{3^2} \cdot \cancel{5} \cdot \frac{1}{\cancel{3}} \cdot \frac{2^2}{\cancel{5}} \\
&= 2^5 \cdot 3 = 32 \cdot 3 = 96
\end{aligned}
$$

<u>Notation:</u> Let $n \in \mathbb{Z}$, $n \geq 2$.

Let $\bar{a} \in \mathbb{Z}_n^{\times}$.

Suppose $\mathbb{Z}_n^{\times} = \{ \overline{x_1}, \overline{x_2}, \ldots, \overline{x_{\varphi(n)}} \}$

Define $\bar{a} \cdot \mathbb{Z}_n^{\times}$ to be the set

$$\bar{a} \cdot \mathbb{Z}_n^{\times} = \{ \bar{a} \cdot \overline{x_1}, \bar{a} \cdot \overline{x_2}, \ldots, \bar{a} \cdot \overline{x_{\varphi(n)}} \}$$

<u>Ex:</u> $n = 10$

$$\mathbb{Z}_{10}^{\times} = \{ \bar{1}, \bar{3}, \bar{7}, \bar{9} \}$$

$\bar{a} = \bar{7}$

$$\begin{aligned} \bar{7} \cdot \mathbb{Z}_{10}^{\times} &= \{ \bar{7} \cdot \bar{1}, \bar{7} \cdot \bar{3}, \bar{7} \cdot \bar{7}, \bar{7} \cdot \bar{9} \} \\ &= \{ \bar{7}, \overline{21}, \overline{49}, \overline{63} \} \\ &= \{ \bar{7}, \bar{1}, \bar{9}, \bar{3} \} = \mathbb{Z}_{10}^{\times} \end{aligned}$$

$\overline{21} = \bar{1}$
$\overline{49} = \bar{9}$
$\overline{63} = \bar{3}$

Theorem: Let $n \in \mathbb{Z}$ with $n \geq 2$.
Let $\overline{a} \in \mathbb{Z}_n^{\times}$.
Then $\overline{a} \cdot \mathbb{Z}_n^{\times} = \mathbb{Z}_n^{\times}$

proof: Let $\mathbb{Z}_n^{\times} = \{ \overline{x_1}, \overline{x_2}, \ldots, \overline{x_{\varphi(n)}} \}$

(Part 1) Let's show $\overline{a} \cdot \mathbb{Z}_n^{\times} \subseteq \mathbb{Z}_n^{\times}$.

Let $\overline{y} \in \overline{a} \cdot \mathbb{Z}_n^{\times}$.
Then, $\overline{y} = \overline{a} \cdot \overline{x_i}$ where $1 \leq i \leq \varphi(n)$.
We showed previously that $\mathbb{Z}_n^{\times}$ is closed under multiplication.
Since $\overline{a}$ and $\overline{x_i}$ are in $\mathbb{Z}_n^{\times}$ so is $\overline{y} = \overline{a} \cdot \overline{x_i}$.
So, $\overline{y} \in \mathbb{Z}_n^{\times}$.
Thus, $\overline{a} \cdot \mathbb{Z}_n^{\times} \subseteq \mathbb{Z}_n^{\times}$.

(Part 2) Let's show $\mathbb{Z}_n^\times \subseteq \overline{a} \cdot \mathbb{Z}_n^\times$

Pick some $\overline{x_i} \in \mathbb{Z}_n^\times$ where $1 \leq i \leq \varphi(n)$.

We want to show $\overline{x_i} \in \overline{a} \cdot \mathbb{Z}_n^\times$.

Since $\overline{a} \in \mathbb{Z}_n^\times$ we know $\overline{a}^{-1} \in \mathbb{Z}_n^\times$.

Since $\mathbb{Z}_n^\times$ is closed under multiplication we know $\overline{a}^{-1} \cdot \overline{x_i} \in \mathbb{Z}_n^\times$.

Thus,

$$
\begin{aligned}
\overline{x_i} &= \overline{1} \cdot \overline{x_i} = \overline{a} \cdot \overline{a}^{-1} \overline{x_i} \\
&= \overline{a} \cdot \underbrace{(\overline{a}^{-1} \cdot \overline{x_i})}_{\text{in } \mathbb{Z}_n^\times} \in \overline{a} \cdot \mathbb{Z}_n^\times
\end{aligned}
$$

So, $\mathbb{Z}_n^\times \subseteq \overline{a} \cdot \mathbb{Z}_n^\times$.

By Part 1 and Part 2,

$$\overline{a} \cdot \mathbb{Z}_n^\times = \mathbb{Z}_n^\times \qquad \blacksquare$$

Summary so far:

- $\varphi(n) = |\mathbb{Z}_n^\times|$

- $\bar{a} \in \mathbb{Z}_n^\times$

$$\boxed{\bar{a}\,\mathbb{Z}_n^\times = \mathbb{Z}_n^\times}$$

where

$$\mathbb{Z}_n^\times = \{\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{\varphi(n)}\}$$

$$\bar{a}\,\mathbb{Z}_n^\times = \{\bar{a}\bar{x}_1, \bar{a}\bar{x}_2, \ldots, \bar{a}\bar{x}_{\varphi(n)}\}$$

Euler's Theorem:

Let $n \in \mathbb{Z}$ with $n \geq 2$.
Let $\overline{a} \in \mathbb{Z}_n^\times$.
Then in $\mathbb{Z}_n^\times$ we have

$$\overline{a}^{\varphi(n)} = \overline{1}$$

proof after examples

$\boxed{\text{Ex:}}$ Consider $\mathbb{Z}_{360}^\times$.

We calculated last time that $\varphi(360) = |\mathbb{Z}_{360}^\times| = 96$.
Note that $\gcd(7, 360) = 1$.
Thus, $\overline{7} \in \mathbb{Z}_{360}^\times$. Euler's thm says $\overline{7}^{96} = \overline{1}$ in $\mathbb{Z}_{360}^\times$.

Same: $7^{96} \equiv 1 \pmod{360}$

<u>Ex:</u> $\mathbb{Z}_{10}^{\times} = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$

$\varphi(10) = |\mathbb{Z}_{10}^{\times}| = 4$

Euler says:

$$\bar{1}^4 = \bar{1}$$

$$\bar{3}^4 = \bar{1}$$

$$\bar{7}^4 = \bar{1}$$

$$\bar{9}^4 = \bar{1}$$

in $\mathbb{Z}_{10}^{\times}$.

Proof of Euler's Theorem:

Let $\mathbb{Z}_n^\times = \{ \overline{x_1}, \overline{x_2}, \ldots, \overline{x_{\varphi(n)}} \}$

and let $\overline{a} \in \mathbb{Z}_n^\times$.

Then because $\overline{a} \cdot \mathbb{Z}_n^\times = \mathbb{Z}_n^\times$ we have

$$\underbrace{(\overline{a}\,\overline{x_1})(\overline{a}\,\overline{x_2})\cdots(\overline{a}\,\overline{x_{\varphi(n)}})}_{\text{elements of } \overline{a}\mathbb{Z}_n^\times \text{ multiplied together}} = \underbrace{\overline{x_1}\,\overline{x_2}\cdots\overline{x_{\varphi(n)}}}_{\text{elements of } \mathbb{Z}_n^\times \text{ multiplied together}}$$

Hence

$$\overline{a}^{\varphi(n)}\left[\overline{x_1}\,\overline{x_2}\cdots\overline{x_{\varphi(n)}}\right] = \overline{x_1}\,\overline{x_2}\cdots\overline{x_{\varphi(n)}}$$

Since each $\overline{x_i}$ is in $\mathbb{Z}_n^\times$ we know $\overline{x_i}^{-1}$ exists.

Multiplying by these multiplicative inverses we get that

$$\underbrace{\overline{a}^{\varphi(n)}\left[\overline{x}_1\overline{x}_2\cdots\overline{x}_{\varphi(n)}\right]\overline{x}_1^{-1}\,\overline{x}_2^{-1}\cdots\overline{x}_{\varphi(n)}^{-1}}_{\overline{1}}$$

$$= \underbrace{\left[\overline{x}_1\overline{x}_2\cdots\overline{x}_{\varphi(n)}\right]\overline{x}_1^{-1}\,\overline{x}_2^{-1}\cdots\overline{x}_{\varphi(n)}^{-1}}_{\overline{1}}$$

Thus, $\overline{a}^{\varphi(n)} = \overline{1}$ in $\mathbb{Z}_n^\times$ ∎

$\boxed{\text{4550 proof:}}$ $\mathbb{Z}_n^\times$ is a group under multiplication. [Thm: If G is a group and $x \in G$, then $x^{|G|} = e$]

Thus, $\overline{a}^{|\mathbb{Z}_n^\times|} = \overline{1}$ when $\overline{a} \in \mathbb{Z}_n^\times$ ∎

Corollary (Fermat's theorem)

If p is a prime and $\overline{a} \in \mathbb{Z}_p^{\times}$, then

$$\overline{a}^{\,p-1} = \overline{1} \quad \text{in } \mathbb{Z}_p^{\times}.$$

proof:

Since p is prime $\varphi(p) = p-1$ and so by Euler

$$\overline{a}^{\,p-1} = \overline{a}^{\,\varphi(p)} = \overline{1} \quad \text{in } \mathbb{Z}_p^{\times}.$$

$\blacksquare$

[It's a special case of Euler's theorem]

HW 5

⑨ Reduce $\overline{5}^{127}$ in $\mathbb{Z}_{12}$

Note that $\gcd(5,12)=1$.

Thus, $\overline{5} \in \mathbb{Z}_{12}^{\times}$.

In fact,

$$\mathbb{Z}_{12}^{\times} = \{ \overline{1}, \overline{5}, \overline{7}, \overline{11} \}$$

So, $\varphi(12) = |\mathbb{Z}_{12}^{\times}| = 4$

Euler says that

$$\overline{5}^{4} = \overline{5}^{\varphi(12)} = \overline{1}$$

in $\mathbb{Z}_{12}^{\times}$.

Note that

$$127 = 4(31) + 3$$

$$\begin{array}{r} 31 \\ 4\overline{)127} \\ -12 \\ \hline 7 \\ -4 \\ \hline 3 \end{array}$$

Thus,

$$\overline{5}^{127} = \overline{5}^{4 \cdot 31 + 3}$$

$$= \left(\overline{5}^{4}\right)^{31} \cdot \overline{5}^{3}$$

$$= \left(\overline{1}\right)^{31} \cdot \overline{5}^{3}$$

$$= \overline{5}^{3} = \overline{5} \cdot \overline{5} \cdot \overline{5}$$

$$= \overline{25} \cdot \overline{5} = \overline{1} \cdot \overline{5} = \overline{5}$$

$25 \equiv 1 \pmod{12}$

$\overline{25} = \overline{1}$ in $\mathbb{Z}_{12}$

So, $\overline{5}^{127} = \overline{5}$ in $\mathbb{Z}_{12}$.

Def: Let $n \in \mathbb{Z}$ with $n \geq 2$. We say that $\bar{g} \in \mathbb{Z}_n^\times$ is a <u>primitive root</u> for $\mathbb{Z}_n^\times$ if every element $\bar{y}$ in $\mathbb{Z}_n^\times$ can be expressed in the form $\bar{y} = \bar{g}^k$ where k is a positive integer.

<u>4550 language:</u>
If $\mathbb{Z}_n^\times$ is cyclic, then a primitive root is a generator for $\mathbb{Z}_n^\times$.

Ex: $\mathbb{Z}_{10}^{\times} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$

Is $\overline{3}$ a primitive root?

$\overline{3}^1 = \overline{3}$

$\overline{3}^2 = \overline{9}$

$\overline{3}^3 = \overline{27} = \overline{7}$

$\overline{3}^4 = \overline{3} \cdot \overline{3}^3 = \overline{3} \cdot \overline{7} = \overline{21} = \overline{1}$

So, every element of $\mathbb{Z}_{10}^{\times}$ can be written as a positive power of 3.

The positive powers of $\overline{3}$ generate all of $\mathbb{Z}_{10}^{\times}$

Yes, $\overline{3}$ is a primitive root of $\mathbb{Z}_{10}^{\times}$.

Is $\overline{7}$ a primitive root of $\mathbb{Z}_{10}^{\times}$?

$\overline{1}$ $\overline{42}$

$\overline{7}^1 = \boxed{\overline{7}}$

$\overline{7}^2 = \overline{49} = \boxed{\overline{9}}$

$\overline{7}^3 = \overline{7} \cdot \overline{7}^2 = \overline{7} \cdot \overline{9} = \overline{63} = \boxed{\overline{3}}$

$\overline{7}^4 = \boxed{\overline{1}}$

Euler
$\varphi(10) = |\mathbb{Z}_{10}^{\times}| = 4$

Yes, $\overline{7}$ is a primitive root of $\mathbb{Z}_{10}^{\times}$, because every element of $\mathbb{Z}_{10}^{\times}$ is equal to a positive power of $\overline{7}$

Note: $\overline{1}$ is not a primitive root since $\overline{1}^k = \overline{1}$ for all k.

Is $\overline{9}$ a primitive root of $\mathbb{Z}_{10}^\times$?

$\overline{9}^1 = \boxed{\overline{9}}$

$\overline{9}^2 = \overline{81} = \boxed{\overline{1}}$

$\overline{9}^3 = \overline{9} \cdot \overline{9}^2 = \overline{9} \cdot \overline{1} = \boxed{\overline{9}}$

$\overline{9}^4 = \overline{9} \cdot \overline{9}^3 = \overline{9} \cdot \overline{9} = \boxed{\overline{1}}$

$\vdots \quad \vdots$

This repeats and you only get $\overline{1}$ and $\overline{9}$ are powers of $\overline{9}$.

Thus, $\overline{9}$ is not a primitive root of $\mathbb{Z}_{10}^\times$.

[$\overline{7}$ and $\overline{3}$ are not powers of $\overline{9}$]

The primitive roots of

$$\mathbb{Z}_{10}^{\times} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$$

are $\overline{3}$ and $\overline{7}$.

Ex: $\mathbb{Z}_8^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$

$\overline{1}^1 = \overline{1}$	$\overline{3}^1 = \overline{3}$	$\overline{5}^1 = \overline{5}$	$\overline{7}^1 = \overline{7}$
$\overline{1}^2 = \overline{1}$	$\overline{3}^2 = \overline{9} = \overline{1}$	$\overline{5}^2 = \overline{25} = \overline{1}$	$\overline{7}^2 = \overline{49} = \overline{1}$
$\overline{1}^3 = \overline{1}$	$\overline{3}^3 = \overline{3}$	$\overline{5}^3 = \overline{5}$	$\overline{7}^3 = \overline{7}$
	$\overline{3}^4 = \overline{1}$	$\overline{5}^4 = \overline{1}$	$\overline{7}^4 = \overline{1}$
$\vdots \quad \vdots$	$\vdots \quad \vdots$	$\vdots \quad \vdots$	$\vdots \quad \vdots$

Each of the above columns repeats over and over and never gives you all of $\mathbb{Z}_n^\times$

None of the elements of $\mathbb{Z}_8^\times$ are primitive roots.

$\mathbb{Z}_8^\times$ has no primitive roots.

4550: $\mathbb{Z}_8^\times$ is not a cyclic group

<u>Theorem:</u> Let p be a prime. Then there exists a primitive root for $\mathbb{Z}_p^\times$.

Moreover, there exist $\varphi(p-1)$ primitive roots in $\mathbb{Z}_p^\times$.

<u>Ex:</u> $\mathbb{Z}_5^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

You can show that $\overline{2}$ and $\overline{3}$ are the primitive roots.

$p=5$ is prime

Note, $\varphi(5-1) = \varphi(4) = |\mathbb{Z}_4^\times|$

$= |\{\overline{1}, \overline{3}\}| = 2.$

<u>Theorem:</u> There exists a primitive root of $\mathbb{Z}_n^\times$ if and only if $n = 2, 4, p^k$, or $2p^\ell$ where p is an odd prime

<u>Ex:</u> $\mathbb{Z}_8^\times$ has no primitive roots because $8 = 2^3$

<u>Ex:</u> $\mathbb{Z}_{12}^\times$ has no primitive roots because $12 = 4 \cdot 3$

<u>Ex:</u> $\mathbb{Z}_{50}^\times$ $50 = 2 \cdot 5^2$ has primitive roots

<u>Ex:</u> $\mathbb{Z}_{125}^\times$ has primitive roots because $125 = 5^3$

(From "Primitive root modulo n" wikipedia article) 48

Finding primitive roots [edit]

No simple general formula to compute primitive roots modulo n is known.[a][b] There are however methods to locate a primitive root that are faster than simply trying out all candidates. If the multiplicative order of a number m modulo n is equal to $\varphi(n)$ (the order of $\mathbb{Z}_n^\times$), then it is a primitive root. In fact the converse is true: If m is a primitive root modulo n, then the multiplicative order of m is $\varphi(n)$. We can use this to test a candidate m to see if it is primitive.

First, compute $\varphi(n)$. Then determine the different prime factors of $\varphi(n)$, say p_1, ..., p_k. Finally, compute

$$m^{\varphi(n)/p_i} \bmod n \qquad \text{for } i = 1, \ldots, k$$

using a fast algorithm for modular exponentiation such as exponentiation by squaring. A number m for which these k results are all different from 1 is a primitive root.

The number of primitive roots modulo n, if there are any, is equal to[8]

$$\varphi\left(\varphi(n)\right)$$

since, in general, a cyclic group with r elements has $\varphi(r)$ generators. For prime n, this equals $\varphi(n-1)$, and since $n/\varphi(n-1) \in O(\log\log n)$ the generators are very common among {2, ..., n−1} and thus it is relatively easy to find one.[9]

If g is a primitive root modulo p, then g is also a primitive root modulo all powers p^k unless $g^{p-1} \equiv 1 \pmod{p^2}$; in that case, $g + p$ is.[10]

If g is a primitive root modulo p^k, then either g or $g + p^k$ (whichever one is odd) is a primitive root modulo $2p^k$.[10]

Finding primitive roots modulo p is also equivalent to finding the roots of the $(p - 1)$ st cyclotomic polynomial modulo p.

Order of magnitude of primitive roots [edit]

The least primitive root g_p modulo p (in the range 1, 2, ..., $p - 1$) is generally small.

Upper bounds [edit]

Burgess (1962) proved[11] that for every $\varepsilon > 0$ there is a C such that $g_p \leq C\,p^{\frac{1}{4}+\epsilon}$.

Grosswald (1981) proved[11] that if $p > e^{e^{24}}$, then $g_p < p^{0.499}$.

Carella (2015) proved[12] that there is a $C > 0$ such that $g_p \leq C\,p^{5/\log\log p}$ for all sufficiently large primes $p > 2$.

Shoup (1990, 1992) proved,[13] assuming the generalized Riemann hypothesis, that $g_p = O(\log^6 p)$.

Lower bounds [edit]

Fridlander (1949) and Salié (1950) proved[11] that there is a positive constant C such that for infinitely many primes $g_p > C \log p$.

It can be proved[11] in an elementary manner that for any positive integer M there are infinitely many primes such that $M < g_p < p - M$.

Applications [edit]

A primitive root modulo n is often used in cryptography, including the Diffie–Hellman key exchange scheme. Sound diffusers have been based on number-theoretic concepts such as primitive roots and quadratic residues.[14][15]

Artin's conjecture on primitive roots

(From wikipedia) 49

From Wikipedia, the free encyclopedia

This page discusses a conjecture of Emil Artin on primitive roots. For the conjecture of Artin on L-functions, see Artin L-function.

In number theory, **Artin's conjecture on primitive roots** states that a given integer *a* that is neither a perfect square nor −1 is a primitive root modulo infinitely many primes *p*. The conjecture also ascribes an asymptotic density to these primes. This conjectural density equals Artin's constant or a rational multiple thereof.

The conjecture was made by Emil Artin to Helmut Hasse on September 27, 1927, according to the latter's diary. The conjecture is still unresolved as of 2020. In fact, there is no single value of *a* for which Artin's conjecture is proved.

Contents [hide]

Formulation [edit]

Let a be an integer that is not a perfect square and not −1. Write $a = a_0b^2$ with a_0 square-free. Denote by $S(a)$ the set of prime numbers p such that a is a primitive root modulo p. Then the conjecture states

1. $S(a)$ has a positive asymptotic density inside the set of primes. In particular, $S(a)$ is infinite.
2. Under the conditions that a is not a perfect power and that a_0 is not congruent to 1 modulo 4 (sequence A085397 in the OEIS), this density is independent of a and equals **Artin's constant**, which can be expressed as an infinite product

$$C_{\text{Artin}} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136\ldots$$ (sequence A005596 in the OEIS).

Similar conjectural product formulas [1] exist for the density when a does not satisfy the above conditions. In these cases, the conjectural density is always a rational multiple of C_{Artin}.

Example [edit]

For example, take $a = 2$. The conjecture claims that the set of primes p for which 2 is a primitive root has the above density C_{Artin}. The set of such primes is (sequence A001122 in the OEIS)

$S(2) = \{3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179, 181, 197, 211, 227, 269, 293, 317, 347, 349, 373, 379, 389, 419, 421, 443, 461, 467, 491, \ldots\}$.

It has 38 elements smaller than 500 and there are 95 primes smaller than 500. The ratio (which conjecturally tends to C_{Artin}) is 38/95 = 2/5 = 0.4.

Partial results [edit]

In 1967, Christopher Hooley published a conditional proof for the conjecture, assuming certain cases of the generalized Riemann hypothesis.[2]

Without the generalized Riemann hypothesis, there is no single value of *a* for which Artin's conjecture is proved. D. R. Heath-Brown proved (Corollary 1) that at least one of 2, 3, or 5 is a primitive root modulo infinitely many primes *p*.[3] He also proved (Corollary 2) that there are at most two primes for which Artin's conjecture fails.